## REMARKS

Claims 1, 3, 4, 6-11, 13-16, and 18-24 are pending and stand finally rejected. Claim 21 is canceled herein. Claims 1, 3, 4, 6-11, 13-16, 18-20 and 22-24 are pending upon entry of this amendment.

## Objection to the Specification

The specification stands objected to for typographical errors. Applicants have amended the specification as suggested by the Examiner.

## 35 USC § 103 Rejections

Claims 1, 3, 4, 6-11, 13-16, 18, 19, 21, 23 and 24 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Applicant admitted prior art in view of Ramarao (U.S. Publication No. 2004/0199647), and further in view of Gruper (U.S. Patent No. 7,047,369). Claim 20 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Applicant admitted prior art in view of Ramarao in view of Gruper, and further in view of Yaeger (US Patent No. 5,768,422). Claim 22 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Applicant admitted prior art in view of Ramarao in view of Gruper, and further in view of Yaeger. Applicants respectfully traverse these rejections.

Independents claims 1, 16, and 20 recite elements related to training a database intrusion detection system. For example, independent claim 1 recites:

> observing, in real time, commands that are accessing the database during a training phase;
> grouping the commands into categories;
> performing a statistical analysis of the categories;

deriving from said commands, in real time, a set of acceptable commands; and
ending the training phase responsive to the statistical analysis.

Thus, independent claim 1 recites, *inter alia*, "grouping the commands into categories…", "performing a statistical analysis of the categories," deriving "a set of acceptable commands," and "ending the training phase responsive to the statistical analysis." Independent claims 16 and 20 recite similar limitations.

The references, whether considered individually or combined, do not disclose or suggest the claimed invention. The alleged admitted prior art merely shows the existence of database intrusion detection systems.

Ramarao, in turn, describes a software environment in which a message requesting an action is received from a node. A determination is made that the action is not permitted in the software environment and the requested action is prevented from occurring. *See* Ramarao, Abstract.

In rejecting claim 1, the Examiner argues that Ramarao discloses grouping commands into categories at ¶ [0032]. *See* Final Office Action (8/25/08), p. 6. This portion of the reference discloses that multiple nodes can exist in a client environment and that access control software can be implemented against each node in the client environment to restrict one node from initiating remote actions and/or operator initiated actions onto another node. The disclosed access control restrictions can be granular, and can be set based on parameters to the remote actions:

> Additionally, the enforcement can be made granular in terms of what exact remote actions can be initiated. The parameters to those remote actions can be set to be validated, if they can be compared against any local OVO environment variable, string matched, or just **configured as variable**. In one embodiment, only the actions that are defined in the configuration file of access control software 460 are allowed, all other actions are prevented from occurring.

(Ramarao, ¶ [0032], emphasis added). The Examiner asserts that this text indicates that commands are generalized using variables and grouped according to the types of commands. Thus, the alleged categories in Ramarao are formed from enforcement restrictions where parameters of remote actions are specified as variable.

The Examiner acknowledges that Ramarao does not disclose that commands are observed in real time before deriving the set of acceptable commands. If fact, Ramarao explicitly requires that the acceptable commands be specified *a priori*. At ¶¶ [0055-56], Ramarao describes how a configuration file can be configured to allow specific authorized actions. It is this configuration file that is referenced in ¶ [0032]. Therefore, the alleged groups identified by the Examiner in Ramarao, and the acceptable commands, are explicitly specified before any commands are received.

The Examiner implicitly acknowledges that Ramarao does not disclose performing a statistical analysis of the alleged categories and asserts that this deficiency is remedied by Gruper. Gruper describes an operating environment that prevents unacceptable application behavior by defining activity behavior as either acceptable or suspect. *See* Gruper, Abstract. The Examiner argues that "Gruper explicitly discloses several statistical methods by which the duration of the training phase may be determined" at 2:50-63. *See* Final Office Action (8/25/08), p. 3. This portion of the reference is as follows:

> In embodiments the step of querying may only be carried out for **a limited period of time**. This may be literally a predetermined time from installation of any given program or it may be a predetermined time measured only whilst the new program is running. Alternatively a program may be run in this learning mode until the next occasion upon which the computer is reset. Then again in one embodiment **a predetermined number of operations of the new program is counted through**, and once that number is reached learning mode is ended. Other forms of limitation of the learning mode will suggest themselves to the skilled person and all of these are viable alternatives that could

> provide useful embodiments of the invention. As an alternative it is possible not to set a limit on the length of the learning mode.

(emphasis added).

The text relied upon by the Examiner describes multiple ways of ending the learning mode. Several of the ways are dependent upon only elapsed time, and cannot reasonably be said to involve a statistical analysis of categories. Another way of ending the learning mode is waiting until the computer "is reset" and this method also does not involve a statistical analysis of categories. The final way of ending the learning mode disclosed in the portion cited by the examiner is counting a "predetermined number of operations" and this technique must be the alleged statistical method referenced by the Examiner.

Therefore, the Examiner's rejection is based on a combination of alleged admitted prior art, Ramarao, and Gruper where a prior art database IDS is modified by Ramarao to allow previously-authorized commands having variable parameters, and then a training phase is run until a predetermined number of commands are received as taught by Gruper.

However, the combination proposed by the Examiner would not lead to the claimed invention. Ramarao requires that acceptable commands be specified in advance. Gruper, in turn, simply teaches counting the number of commands received. The resulting combination is a DIDS in which acceptable commands are specified in advance, and then a training phase is ended when a predetermined number of acceptable commands is received.

Such a combination would not "allow a system to gradually build up knowledge of what actions are and are not to be allowed" as stated by the Examiner. Rather, such a system would not build any knowledge as to what commands are allowed since the **authorized commands are already known**. The combination proposed by the Examiner thus changes the principle of operation of the references and is inoperable for the purpose

asserted by the Examiner. Furthermore, the combination would not derive the set of acceptable commands in real time as claimed. For at least these reason, a person of ordinary skill in the art considering the cited references individually or in the combination proposed by the Examiner would not find the claimed invention obvious.

Yaeger does not remedy the deficiencies of Ramarao, Gruper, and the alleged admitted prior art. Yaeger describes a statistical classifier for pattern recognition that is trained to recognize negative and positive patterns that are properly associated with desired output classes. *See* Yaeger, Abstract. However, Yaeger does not disclose or suggest grouping commands into categories or performing a statistical analysis of the categories as recited by the independent claims.

Accordingly, Applicants respectfully submit that the cited references do not teach or suggest every element of independent claims 1, 16, and 20. Therefore, a person of ordinary skill in the art would considering the references either individually or in combination would not find the claimed invention obvious. The dependent claims not mentioned above incorporate the elements of their base claims and are therefore not obvious for at least the same reasons.

## CONCLUSION

Should the Examiner wish to discuss the above amendments and remarks, or if the Examiner believes that for any reason direct contact with Applicants' representative would help to advance the prosecution of this case to finality, the Examiner is invited to telephone the undersigned at the number given below. In the event that the Examiner maintains the rejections, **Applicants respectfully request that the Examiner enter this amendment in order to place the application in better form for appeal.**

Respectfully submitted,

CAREY NACHENBERG ET AL.

Dated: October 27, 2008

By: /Brian Hoffman/
Brian M. Hoffman, Reg. No. 39, 713
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350